TD SYNNEX

Security Solutions

Securitywoordenboek

De belangrijkste terminologie op een rij

Security kent een geheel eigen vaktaal. Bovendien komen er regelmatig nieuwe termen bij. Duizelt het je? Geen zorgen, in dit securitywoordenboek hebben we de meest voorkomende termen verzameld en uitgelegd.

ADVANCED PERSISTENT THREAT (APT)

Geavanceerde aanhoudende bedreigingen (APT's): Geavanceerde en gerichte cyberaanvallen die gedurende een langere periode worden uitgevoerd door bekwame tegenstanders. APT's omvatten vaak meerdere aanvalsvectoren, social engineering en geavanceerde technieken om systemen te infiltreren, gegevens te extraheren of blijvende toegang te verkrijgen.

ANTIVIRUSSOFTWARE

Antivirussoftware beschermt endpoints tegen virussen en andere schadelijke software (malware). Dat gebeurt voornamelijk aan de hand van een handtekeningendatabase en/of gedragsherkenning (heuristiek). Doorgaans zijn dergelijke oplossingen onderdeel van een zogeheten 'security suite', die bijvoorbeeld ook een spamfilter bevat en bescherming tegen onder andere dns-gebaseerde bedreigingen biedt.

APPLICATIEBLACKLISTING

Een oplossing voor applicatieblacklisting blokkeert de uitvoer van specifieke applicaties. In de praktijk kan dat een lijst zijn van software die een organisatie ongepast of onveilig acht op de werkvloer. Ook anti-malwareapplicaties werken volgens dit principe.

APPLICATIEWHITELISTING

Een oplossing voor applicatiewhitelisting staat enkel de uitvoering van een specifieke, voorgedefinieerde lijst van applicaties op endpoints toe. Op die manier voorkomt een dergelijke oplossing dat gebruikers software installeren en uitvoeren zonder toestemming van de IT-afdeling. Het voorkomt ook dat malware de kans krijgt schade aan te richten.

AUTHENTICATIE

Het proces van verificatie van de identiteit van een persoon of apparaat om toegang te verlenen tot specifieke bronnen of systemen.
Anders gezegd geeft authenticatie antwoord op de vraag of iemand ook daadwerkelijk is die hij/zij zegt te zijn.

Voor security is authenticatie erg belangrijk. Het voorkomt dat onbevoegden toegang krijgen tot data, systemen en applicaties. Authenticatie kan plaatsvinden op allerlei manieren. Via bijvoorbeeld een wachtwoord en een gebruikersnaam, een vingerafdrukscan, een irisscan, stemherkenning, een token of een combinatie van meerdere van deze factoren.

AUTORISATIE

Autorisatie is het proces waarbij een systeem rechten toekent aan gebruikers. In de praktijk zijn dat bijvoorbeeld lees- en/of schrijfrechten voor gegevens, toegangsrechten tot een netwerk of het recht op uitvoering van een bepaalde applicatie.

ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

Algemene verordening gegevensbescherming is de Nederlandse term voor de General Data Protection Regulation (GDPR), een Europese verordening die regels voor de verwerking van persoonsgegevens standaardiseert. De AVG bepaalt onder meer dat persoonsgegevens uitsluitend verwerkt mogen worden in overeenstemming met de wet en verzameld met een gerechtvaardigd doel. Ook moeten gegevens adequaat zijn beveiligd en dienen zo min mogelijk data te worden verzameld. In Nederland ziet de AP (Autoriteit Persoonsgegevens) toe op een correcte naleving ervan.

APPLICATION PROGRAMMING INTERFACE (API)

Een Application Programming Interface is een interface die het mogelijk maakt dat twee applicaties of computerprogramma's met elkaar communiceren. Iedereen heeft er eigenlijk elke dag mee te maken, want zodra er twee systemen met elkaar in verbinding staan is er een API aan het werk.

BACK-UP

Een back-up is een kopie van fysieke of virtuele bestanden of databases op een secundaire locatie. Gaan bij een incident de originele data (deels) verloren, dan kan de organisatie terugvallen op deze veiliggestelde kopie. Bij zo'n incident kunt u denken aan fysieke schade door een natuurramp, het (onopzettelijk) wissen van gegevens door medewerkers, het gijzelen, vernietigen of beschadigen van gegevens door hackers of gegevensverlies door falende hardware.

BEDREIGING VAN BINNENUIT

Een interne bedreiging door personen binnen een organisatie die geautoriseerde toegang hebben tot systemen en gegevens, maar hun privileges misbruiken voor persoonlijk gewin, spionage of sabotage. Bedreigingen van binnenuit kunnen onbedoeld of kwaadaardig zijn.

BITLOCKER

BitLocker is een oplossing van Microsoft voor bestandsversleuteling. BitLocker is geïntegreerd in Windows Vista, Windows Server 2008, Windows 7, Windows 8 en Windows 10. De oplossing maakt gebruik van 128-bits AES-encryptie.

BUSINESS EMAIL COMPROMISE (BEC)

Business Email Compromise is een vorm van cybercriminaliteit waarbij fraudeurs ongeoorloofde toegang krijgen tot het e-mailsysteem van een bedrijf om werknemers te misleiden tot schadelijke handelingen.

Deze acties kunnen bestaan uit het overmaken van geld, het delen van gevoelige informatie of het uitvoeren van frauduleuze transacties. BEC-aanvallen omvatten vaak social engineering-tactieken om werknemers te laten geloven dat het verzoek of de communicatie legitiem is. Het doel van BEC is het vertrouwen binnen een organisatie te misbruiken om financiële fraude te plegen of toegang te krijgen tot vertrouwelijke gegevens.

BLACK HAT

Met de term 'black hat' wordt in de securitywereld een persoon aangeduid met kwade bedoelingen. Vaak gaat het om een hacker, of bijvoorbeeld een ontwikkelaar van malware. Het tegenovergestelde van black hat is white hat.

BOTNET

Een botnet is een netwerk van door hackers overgenomen systemen. Dat kunnen traditionele laptops, servers en werkstations zijn, maar bijvoorbeeld ook Internet of Things (IoT)-apparaten. Botnets worden veel ingezet voor het uitvoeren van een DDoS-aanval.

BRING YOUR OWN ENCRYPTION (BYOE)

Bring your own encryption is een beveiligingsmodel voor cloudcomputing. Hiermee kunnen eindklanten die clouddiensten afnemen van hun eigen encryptiesoftware gebruikmaken en hun eigen encryptiesleutels beheren. Bij BYOE draaien eindklanten hun encryptiesoftware als gevirtualiseerde instance naast de business applicatie in het datacenter van de cloudprovider. Die applicatie is vervolgens zo geconfigureerd dat de encryptiesoftware alle gegevensverwerking voor zijn rekening neemt.

De versleutelde versie van de gegevens wordt naar de fysieke dataopslag van de clouddienstverlener weggeschreven.

BUSINESS CONTINUITY (BC) EN DISASTER RECOVERY (DR)

Business continuity en disaster recovery zijn verzameltermen voor alle processen en oplossingen van een organisatie om operationeel te blijven na een ongunstige gebeurtenis. Het doel van BC/DR is om risico's te beperken en een organisatie zo dicht mogelijk bij de normale gang van zaken te brengen na een (cyber)incident

CHIEF INFORMATION SECURITY OFFICER (CISO)

De chief information security officer is de persoon die binnen een organisatie verantwoordelijk is voor de processen rondom de beveiliging van informatie. Hij of zij implementeert het informatiebeveiligingsbeleid en houdt er toezicht op. Een belangrijke doelstelling van de CISO is het voorkomen van securityincidenten en het beperken van de impact ervan.

CLOUD ACCESS SECURITY BROKER (CASB)

Cloud Access Security Broker is een beveiligingsoplossing die organisaties helpt beveiligingsbeleid af te dwingen en inzicht in en controle over hun in clouddiensten opgeslagen gegevens te krijgen. Het fungeert als tussenpersoon tussen de organisatie en de aanbieder van clouddiensten en biedt verschillende functionaliteiten.

Zoals gegevensversleuteling, toegangscontrole, bescherming tegen bedreigingen en compliancebewaking om een veilig gebruik van cloudapplicaties te waarborgen.

CLOUDENCRYPTIE

Cloudencryptie is een dienst van cloudproviders waarbij data met algoritmes worden versleuteld en in de cloud worden opgeslagen. Cloudencryptie is bijna hetzelfde als 'normale' encryptie. Een belangrijk verschil is dat de klant zich moet verdiepen in de policy's en procedures van de provider. Het encryptieniveau moet namelijk passen bij de gevoeligheid van de data.

CLOUDSECURITY

Cloudsecurity is de beveiliging van data die in de cloud staan en cloudgebaseerde systemen en infrastructuur. Het omvat een breed scala aan beleidsregels, technologieën en applicaties op het gebied van databeveiliging, toegangsbeheer, compliance en privacybescherming. Aangezien cybercriminelen zich steeds vaker richten op de cloud, kunnen organisaties die (deels) in de cloud werken niet zonder solide cloudsecurity.

COMPUTER EXPLOIT

Een computer exploit of exploit is een aanval op een computersysteem waarbij misbruik wordt gemaakt van een kwetsbaarheid in dat systeem. Dit kan bijvoorbeeld een zwakke plek in een besturingssysteem, een applicatie of plug-in zijn. Vaak rolt de softwareleverancier een fix of patch uit om de kwetsbaarheid te dichten. De verantwoordelijkheid om de patch te downloaden en installeren ligt bij de gebruiker.

CONTAINER NETWORK APPLICATION POLICY (CNAPP)

Container Network Application Policy verwijst naar het beleidskader en de reeks technologieën die worden gebruikt om het netwerk- en beveiligingsbeleid voor gecontaineriseerde toepassingen te beheren. Aangezien containers steeds populairder zijn geworden voor het implementeren en schalen van toepassingen, biedt CNAPP een manier om netwerkconnectiviteit, segmentatie en beveiligingsregels voor gecontaineriseerde werklasten te definiëren en af te dwingen, waardoor efficiënte en veilige communicatie binnen containerclusters mogelijk wordt.

CREDENTIAL STUFFING

Credential stuffing is een cyberaanvalsmethode waarbij aanvallers lijsten met gecompromitteerde gebruikersgegevens gebruiken om in te breken in een systeem. De aanval maakt gebruik van bots voor automatisering en schaalvergroting en is gebaseerd op de veronderstelling dat veel gebruikers gebruikersnamen en wachtwoorden in meerdere diensten hergebruiken.

CYBERCRIMINALITEIT

Cybercriminaliteit of cybercrime is een verzamelterm voor alle illegale activiteit waarbij gebruik wordt gemaakt van digitale middelen zoals computers en netwerken. Soms gaat het om criminele hande lingen waarbij het apparaat het doelwit is, bijvoorbeeld van een aanval met schadelijke software. Maar ook wanneer een device als wapen wordt ingezet – denk hierbij aan DDoS-aanvallen - of om illegaal verkregen data op te slaan, spreken we van cybercrime.

TD SYNNEX

CYBERSECURITY

Cybersecurity is het beschermen van met internet verbonden systemen, hardware, software en data tegen allerlei vormen van cybercriminaliteit, waaronder ransomware- en phishingaanvallen. Cybersecurity omvat diverse disciplines zoals informatie-, netwerk- en applicatiebeveiliging, disaster recovery en awarenesstrainingen. Voor elke discipline zijn er talloze securitymaatregelen en best practices die de kans op een securityincident verkleinen of de impact minimaliseren.

CYBERSECURITY ASSESSMENT TOOL (CSAT)

De Cyber Security Assessment Tool is een compleet helder plan van aanpak om de cyberveiligheid van je organisatie te verbeteren, precies waar dat nodig is. En inclusief duidelijke technologische en procedurele maatregelen, zodat je direct aan de slag kunt en je middelen doelgericht inzet.

CYBER THREAT INTELLIGENCE (CTI)

Cyber Threat Intelligence (CTI) verwijst naar de kennis en inzichten die worden verzameld over potentiële of bestaande cyberdreigingen om organisaties te beschermen tegen kwaadaardige activiteiten. Het gaat om het verzamelen, analyseren en interpreteren van gegevens over cyberdreigingen, waaronder informatie over dreigers, hun tactieken, technieken en procedures. Het helpt bij het verbeteren van het beveiligingsniveau, het nemen van geïnformeerde beslissingen en het uitvoeren van passende tegenmaatregelen om de risico's van cyberdreigingen te beperken.

DARK WEB SECURITY

Dark Web-beveiliging verwijst naar de maatregelen en strategieën die worden toegepast om personen en organisaties te beschermen tegen de risico's van het dark web, een verborgen deel van het internet dat niet wordt geïndexeerd door zoekmachines en vaak wordt geassocieerd met illegale activiteiten. Dark Web security omvat monitoring en het verzamelen van inlichtingen om potentiële bedreigingen te identificeren, het implementeren van robuuste cyberbeveiligingsmaatregelen, het voorlichten van gebruikers over de gevaren van het dark web, en het gebruik van geavanceerde technologieën om potentiële risico's van dit ondergrondse deel van het internet op te sporen en te beperken.

DATA LOSS PREVENTION (DLP)

Data loss prevention is een verzamelterm voor technieken die gevoelige data beschermen, bijvoorbeeld door te voorkomen dat gegevens verwijderd worden of de organisatie per ongeluk verlaten. DLP kan ook verdachte activiteit van kwaadwillende medewerkers detecteren. Functies zoals encryptie (versleuteling) en pseudonimisering (het vervangen van persoonsgegevens door versleutelde gegevens) zijn vaak geïntegreerd in een DLP-oplossing.

DATACENTERSECURITY

Datacentersecurity verwijst naar de fysieke en digitale beveiligingsmaatregelen waarmee een datacenter wordt beschermd tegen externe dreigingen en cyberaanvallen.

In datacenters worden vaak gevoelige of waardevolle data opgeslagen, zoals klantgegevens en intellectueel eigendom. Voorbeelden van securitymaatregelen zijn het beperken van het aantal ingangen (fysiek) en netwerkmonitoring met een security information & event management (SIEM)-oplossing (digitaal).

DATA CLASSIFICATIE

Het toekennen van een waarde aan informatie om te kunnen bepalen welk niveau van bescherming er nodig is. Dataclassificatie is de eerste stap in een beveiligings- of een securitystrategie.

DDOS-AANVAL

Een Distributed Denial-of-Service (DDoS)-aanval is een cyberaanval waarbij criminelen een website of online dienst bestoken met dataverkeer en die tot doel heeft een computersysteem of netwerk onbeschikbaar te maken. Vaak gebruiken ze hiervoor een netwerk van devices die met speciale malware besmet zijn: een botnet. Het primaire doel is meestal verstoring van de dienstverlening, maar een DDoS-aanval kan ook fungeren als afleidingsmanoeuvre.

DEVSECOPS

DevSecOps of SecOps is een managementaanpak waarin de samenwerking tussen de security- en operationele teams centraal staat. Het uitgangspunt van DevSecOps is dat deze teams een gedeelde verantwoordelijkheid dragen en beschikken over dezelfde processen, tools en informatie. Doel hiervan is om te waarborgen dat een hogere uptime en betere prestaties niet ten koste gaan van de security.

E-MAILSPOOFING

E-mailspoofing is het versturen van e-mails vanuit een vervalst e-mailadres dat van iemand anders lijkt te zijn. Op deze manier probeert de cybercrimineel bijvoorbeeld een bank of webwinkel te imiteren. Vaak bevat zo'n e-mail een link naar een malafide website die sterk lijkt op de legitieme website. Het doelwit wordt dan aangemoedigd om daar in te loggen of andere gegevens achter te laten.

ENCRYPTIE

Encryptie of versleuteling is het coderen (versleutelen) van gegevens op basis van een algoritme, zodat ze veilig uitgewisseld kunnen worden over een onveilig communicatiekanaal zoals internet. Met de juiste encryptiesleutels – meestal een reeks van tientallen of honderden tekens – kunnen de versleutelde gegevens vervolgens weer worden gedecodeerd. Er zijn verschillende vormen, zoals symmetrische en asymmetrische encryptie.

END-TO-END ENCRYPTIE (E2EE)

End-to-end encryptie is een vorm van encryptie (versleuteling) die veilige communicatie mogelijk maakt. Met E2EE worden data op het apparaat of systeem van de verzender versleuteld . Alleen de ontvanger kan de data decoderen. Geen enkele andere partij kan de data inzien of manipuleren, of het nou de internetprovider, softwareleverancier of een kwaadwillende hacker is.

ENDPOINTSECURITY

Endpointsecurity is de beveiliging van endpoints. Dit zijn devices zoals smartphones, tablets, laptops, desktop-pc's en servers.

TD SYNNEX

Elk endpoint is een potentiële toegangspoort tot het bedrijfsnetwerk en moet dus beveiligd worden met speciale software. Endpointsecurity is ook van belang als een apparaat wordt gestolen of kwijtraakt. Het zorgt ervoor dat (gevoelige) bedrijfsgegevens dan niet in verkeerde handen vallen.

ETHICAL HACKER

Een ethical hacker of ethische hacker is een securityexpert die zoekt naar zwakke plekken in computersystemen, netwerken en applicaties. Niet om daar misbruik van te maken, maar juist om te voorkomen dat kwaadwillende hackers dat doen. Ethical hackers melden een gevonden kwetsbaarheid op verantwoorde wijze bij de leverancier, fabrikant of opdrachtgever. Deze hackers worden ook wel whitehat-hackers genoemd.

FAST IDENTITY ONLINE (FIDO)

Fast Identity Online is een reeks technologie-agnostische beveiligingsspecificaties voor sterke authenticatie. FIDO is ontwikkeld door de FIDO Alliance, een non-profitorganisatie die authenticatie op de client- en protocollaag wil standaardiseren.

FIREWALL

Een beveiligingsmechanisme dat werkt als een barrière tussen een intern netwerk en externe netwerken, waarbij de stroom netwerkverkeer wordt gecontroleerd op basis van vooraf bepaalde beveiligingsregels. Firewalls beschermen tegen ongeoorloofde toegang en kwaadaardige activiteiten.

GEGEVENSINBREUK

Onbevoegde toegang, openbaarmaking of compromittering van gevoelige informatie, zoals persoonsgegevens, handelsgeheimen of financiële gegevens. Datalekken kunnen leiden tot identiteitsdiefstal, financieel verlies, reputatieschade en juridische gevolgen.

GENERAL DATA PROTECTION REGULATION (GDPR)

De General Data Protection Regulation (GDPR) is een Europese verordening die regels voor de verwerking van persoonsgegevens standaardiseert. In Nederland staat deze verordening bekend als de Algemene verordening gegevensbescherming (AVG). De AVG bepaalt onder meer dat persoonsgegevens uitsluitend verwerkt mogen worden in overeenstemming met de wet en verzameld met een gerechtvaardigd doel. Ook moeten gegevens adequaat zijn beveiligd en dienen zo min mogelijk data te worden verzameld. De Autoriteit Persoonsgegevens (AP) houdt in Nederland toezicht op de naleving van de AVG.

HACKER

Een hacker is iemand die zoekt naar gaten in de beveiliging van onder meer software, firmware, netwerken en infrastructuur. Er zijn verschillende soorten hackers. Zo zoeken zogeheten ethische hackers naar beveiligingsproblemen met als doel de beveiliging te verbeteren. Blackhat-hackers proberen juist misbruik te maken van deze beveiligingsproblemen om bijvoorbeeld systemen, netwerken en apparaten binnen te dringen.

TD SYNNEX

HACKTIVISME

Hacktivisme is het misbruik van computersystemen of netwerken voor een sociaal of politiek gemotiveerd doel. Personen die hiervoor verantwoordelijk zijn staan ook bekend als hacktivisten. Met hun acties proberen hacktivisten de aandacht van het publiek te vestigen op iets wat zij belangrijk vinden. Denk hierbij aan mensenrechten, de vrijheid van meningsuiting of een specifieke misstand. In sommige gevallen tonen hacktivisten op aangevallen websites boodschappen die hun visie onderbouwen.

HONEYPOT

Een honeypot is een systeem dat specifiek is ingericht om cyberaanvallers aan te trekken, te detecteren en te bestuderen. Een honeypot profileert zich daarom op internet als een interessant doelwit, zoals een waardevolle server. Ook kan een honeypot zich presenteren als een systeem dat kwetsbaar is voor een bekend beveiligingslek. Dit maakt het mogelijk in kaart te brengen hoe dit lek in de praktijk wordt misbruikt. Een honeypot kan hiermee waardevolle informatie opleveren en helpen aanvallers buiten écht belangrijke systemen te houden.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity and Access Management is een raamwerk van bedrijfsprocessen, beleidsregels en technologieën dat het beheer van digitale identiteiten faciliteert. De technologie regelt hiermee de toegang tot kritieke informatie binnen hun organisatie. IAM zorgt er onder meer voor dat gevoelige informatie is afgeschermd voor onbevoegden. Het systeem geeft gebruikers echter ook toegang tot data of systemen die zij nodig hebben. De rechten die gebruikers krijgen toegewezen, zijn doorgaans gebaseerd op hun functie binnen de organisatie.

INCIDENT RESPONSE

Incident response is de wijze waarop een organisatie reageert op een cyberaanval en de impact hiervan. Een cyberaanval of -inbraak kan immers nooit 100 procent worden uitgesloten. Incident-response zorgt ervoor dat de organisatie op een securityincident reageert op een wijze die de impact van het incident minimaliseert. Het incident-responseteam werkt aan de hand van een incident-responseplan, waarin instructies zijn omschreven die de organisatie hierbij helpen.

INCIDENTENCODERING

Een techniek die wordt gebruikt om gegevens te versleutelen tijdens een incident response proces om de vertrouwelijkheid en integriteit van gevoelige informatie die mogelijk wordt verzameld of gedeeld tijdens onderzoeken te waarborgen.

INFORMATIEBEVEILIGING

Informatiebeveiliging is het beveiligen van zowel digitale als niet-digitale informatie tegen verkeerd of crimineel gebruik. Onderdeel hiervan is het detecteren, documenteren en tegengaan van cyberdreigingen. Denk echter ook aan het adequaat reageren op aanvallen, met als doel de impact te minimaliseren. Veel grote bedrijven beschikken over een toegewijd securityteam, dat zich volledig richt op IT-beveiliging. Deze groep staat doorgaans onder leiding van de chief information security officer (CISO).

TD SYNNEX

INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)

Beveiligingssystemen die het netwerkverkeer controleren, ongeautoriseerde toegangspogingen detecteren en voorkomen, en waarschuwingen geven of automatische acties ondernemen om potentiële bedreigingen te beperken.

INTRUSION-DETECTIONSYSTEEM (IDS)

Een intrusion-detectionsysteem monitort netwerkverkeer en filtert verdachte activiteiten uit dit verkeer. De oplossing waarschuwt IT- en securityprofessionals hiervoor via een alarmmelding, zodat zij tijdig en gericht actie kunnen nemen. Denk hierbij aan het blokkeren van dataverkeer van en naar een verdacht IP-adres.

INTRUSION-PREVENTIONSYSTEEM (IPS)

Een intrusion-preventionsysteem is een variant op een intrusion-detectionsysteem (IDS). Net als een IDS monitort een IPS netwerkverkeer om verdachte activiteiten op te sporen. Waar een IDS echter waarschuwingen uitstuurt over dergelijke activiteiten, neemt een IPS actief maatregelen om deze tegen te gaan. Denk hierbij aan het blokkeren van potentieel schadelijke datapakketten, zodat deze het netwerk niet meer kunnen bereiken.

IOT-SECURITY

IoT-security is het beveiligen van apparaten en netwerken die deel uitmaken van het Internet of Things (IoT). Het IoT bestaat uit miljarden 'dingen' die via internet met elkaar zijn verbonden. Dit varieert van slimme horloges en fitnessapparatuur tot connected auto's en intelligente koelkasten. Door data door te sturen kan het IoT interessante inzichten opleveren en nieuwe diensten mogelijk maken. Deze connectiviteit maakt IoT-apparaten echter ook kwetsbaar indien deze niet adequaat zijn beveiligd.

KWETSBAARHEIDSBEOORDELING

Proces dat wordt gebruikt om zwakke plekken en kwetsbaarheden in de beveiliging van een systeem of netwerk vast te stellen en te beoordelen.

MALWARE

Malware is de afkorting van "malicious software" en verwijst naar alle kwaadaardige software die is ontworpen om schade toe te brengen aan, misbruik te maken van, of ongeoorloofde toegang te krijgen tot computersystemen. Veel voorkomende types zijn virussen, wormen, Trojaanse paarden en ransomware en spyware. Malware kan gegevens stelen, activiteiten verstoren of aanvallers op afstand bedienen.

MAN-IN-THE-MIDDLE-AANVAL (MitM)

Bij een man-in-the-middle-aanval plaatst een aanvaller zich tussen twee partijen die met elkaar communiceren. Dit maakt het mogelijk dataverkeer te onderscheppen en - indien het verkeer niet is versleuteld - hieruit allerlei informatie te halen. Denk hierbij aan inloggegevens, creditcardgegevens of persoonlijke informatie. De aanvaller kan vaak realtime meekijken, wat het mogelijk maakt gegevens te manipuleren. Onder meer online bankomgevingen en webshops zijn populaire doelwitten voor man-in-themiddle-aanvallen.

TD SYNNEX

MANAGED SECURITY SERVICE PROVIDER (MSSP)

Een managed security service provider is een IT-serviceprovider die beheerde cybersecurityoplossingen levert aan klanten. Denk hierbij aan antivirusoplossingen, intrusion-detectionsystemen en firewalls. Andere voorbeelden zijn virtual private networks en diensten om veilig bestanden te kunnen delen met derden. De oplossingen staan volledig onder beheer van de MSSP, waardoor de klant hier geen omkijken naar heeft. Organisaties bepalen zelf welke securityactiviteiten zij uitbesteden en welke zij liever in eigen beheer houden.

MOBIELE MALWARE

Mobiele malware is kwaadaardige software die specifiek voor mobiele apparaten zoals smartphones, tablets en smartwatches is ontwikkeld. Deze vorm van malware vormt een steeds grotere uitdaging voor organisaties. Zo neemt niet alleen de hoeveelheid mobiele malware toe, maar is dergelijke malware ook steeds geavanceerder. Net als reguliere malware bestaat mobiele malware in verschillende varianten. Zo kan het gaan om spyware of ransomware, maar ook om computerwormen of trojan horses.

MOBILE APPLICATION MANAGEMENT (MAM)

Met Mobile Application Management kunnen IT-beheerders de zakelijke applicaties en bijbehorende data op de smartphones en tablets van werknemers beheren. Applicaties kunnen op afstand worden gepusht, beveiligd, geüpdatet, gemonitord en gewist.

MOBILE DEVICE MANAGEMENT (MDM)

Mobile Device Management is het beheer van mobiele apparaten binnen de ICT-omgeving. Dit doen beheerders vanuit een centrale server, die communiceert met agents op de mobiele apparaten zelf. Ze stellen de beleidsregels in (de policy's) en de agent zorgt ervoor dat het apparaat zich hieraan houdt.

MOBILE SECURITY

Mobile security is de verzamelnaam voor het beveiligen van mobiele apparaten als smartphones en tablets. Deze maken bij bedrijven een steeds groter deel uit van de ICT, mede door Bring Your Own Device (BYOD). Ze zijn echter extra gevoelig voor diefstal en verlies omdat ze zo compact zijn. Het doel van mobile security is om de data op deze apparaten veilig te stellen, ook wanneer het apparaat zoekraakt. Strikt genomen is mobile security alleen bedoeld kleinere, mobiele apparaten die medewerkers altijd op zak hebben. Voor andere endpoints als laptops en desktops wordt gebruikgemaakt van endpointsecurity.

MULTIFACTORAUTHENTICATIE (MFA)

Multifactorauthenticatie is een vorm van authenticatie waarbij een gebruiker meerdere factoren nodig heeft om in te loggen. Die factoren vallen in drie categorieen: wat een gebruiker weet (bijvoorbeeld een gebruikersnaam met wachtwoord), wat een gebruiker heeft (bijvoorbeeld een token of een aparte mobiele applicatie) en wat een gebruiker is (biometrische kenmerken, zoals een vingerafdruk of irisscan). Van multifactorauthenticatie is sprake wanneer minstens twee van deze drie factoren nodig zijn voor een geslaagde inlogpoging.

TD SYNNEX

NETWERKENCRYPTIE

Netwerkencryptie is de versleuteling van gegevens die over een netwerk worden verstuurd. Dit voorkomt dat onbevoegden de data die ze onderscheppen kunnen uitlezen. VPN (Virtual Private Network) is een voorbeeld van netwerkencryptie.

NETWERKSEGMENTATIE

De praktijk van het verdelen van een netwerk in kleinere, geïsoleerde segmenten om potentiële beveiligingslekken te beperken en de laterale beweging van aanvallers. Het verbetert de netwerkbeveiliging door de toegang tot kritieke middelen te beperken.

NETWORK OPERATIONS CENTER (NOC)

Een network operations center is een gecentraliseerde plaats van waaruit beheerders van bedrijfsinformatie technologie (IT) intern - of door derden - toezicht houden op een telecommunicatienetwerk, het controleren en het onderhouden ervan.

NIST SECURITY FRAMEWORK

Het NIST Security Framework, ontwikkeld door het National Institute of Standards and Technology (NIST), is een uitgebreide reeks richtsnoeren en beste praktijken voor het verbeteren van de cyberbeveiliging en het beheren van risico's binnen organisaties. Het kader biedt een flexibele en schaalbare benadering van cyberbeveiliging, waarbij de nadruk ligt op het belang van risicobeoordeling, risicobeheer en voortdurende controle. Het bestaat uit vijf kernfuncties: Identificeren, Beschermen, Opsporen, Reageren en Herstellen.

Deze functies helpen organisaties hun kritieke bedrijfsmiddelen te identificeren, beschermende maatregelen te treffen, cyberbeveiligingsincidenten op te sporen en erop te reageren, en te herstellen van eventuele verstoringen. Het NIST Security Framework dient als waardevol hulpmiddel voor organisaties in verschillende sectoren om hun cyberbeveiligingshouding te verbeteren en een robuust beveiligingsprogramma op te zetten.

PASSWORD/WACHTWOORD

Een wachtwoord (password) is een toegangscode tot een computer, netwerk of programma. Idealiter bestaat zo'n wachtwoord uit een combinatie van kleine letters, hoofdletters, cijfers en speciale symbolen, zoals $ of !.

PASSWORD ATTACK / WACHTWOORDAANVAL

Techniek die worden gebruikt om ongeoorloofde toegang te krijgen tot gebruikersaccounts door zwakke of gestolen wachtwoorden te misbruiken. Dit omvat brute-force aanvallen, woordenboekaanvallen en "credential stuffing", wat het belang onderstreept van het gebruik van sterke, unieke wachtwoorden en multi-factor authenticatie.

PASSWORDLESS AUTHENTICATION/ WACHTWOORDLOZE AUTHENTICATIE

Een authenticatiemethode waarmee een gebruiker toegang kan krijgen tot een toepassing of IT-systeem zonder een wachtwoord in te voeren of beveiligingsvragen te beantwoorden. In plaats daarvan verstrekt de gebruiker een andere vorm van bewijs, zoals een vingerafdruk, proximity badge of hardware token code.

TD SYNNEX

PATCHMANAGEMENT

Het proces van het regelmatig toepassen van updates, patches en fixes op softwaresystemen om kwetsbaarheden in de beveiliging aan te pakken en ervoor te zorgen dat ze up-to-date zijn. Effectief patchmanagement is essentieel voor het in stand houden van een veilige IT-omgeving.

PENTEST (PENETRATIETEST)

Een pentest, een afkorting voor penetratietest, is een procedure waarbij een securityprofessional de ICT-omgeving controleert op kwetsbaarheden. Hij of zij zet verschillende methodes in die cybercriminelen zouden kunnen gebruiken om binnen te komen. Na de pentest schrijft de tester een rapport met resultaten en advies.

PHISHING

Een vorm van social engineering waarbij aanvallers bedrieglijke technieken gebruiken om mensen ertoe te brengen gevoelige informatie, zoals wachtwoorden of creditcardgegevens, vrij te geven door zich via e-mail, telefoon of andere communicatiekanalen voor te doen als een betrouwbare entiteit. In veel gevallen presenteren ze het slachtoffer een link die leidt naar een vervalsing van een inlogpagina van bijvoorbeeld een bank. De gegevens die de gebruiker invult, komen terecht bij de daders, die daarmee bijvoorbeeld rekeningen plunderen of aankopen doen op naam van de gebruiker of diens bedrijf.

PUBLIC KEY INFRASTRUCTURE (PKI)

Een Public Key Infrastructure is een verzameling oplossingen voor het creëren, beheren, beschermen en opslaan van digitale certificaten en openbare sleutels.

Hierdoor is het mogelijk om grote aantallen gebruikers en apparaten snel te voorzien van manieren om zich veilig online kenbaar te maken. Het verkeer tussen gebruiker en systeem kan vervolgens worden versleuteld, zodat de vertrouwelijkheid is gewaarborgd.

PRIVATE CLOUD

Private cloud is een vorm van cloudcomputing waarbij de omgeving op eigen hardware wordt gehost. Dit kunnen servers in het eigen datacenter zijn of servers van een partner, zolang deze hardware niet wordt gedeeld met andere partijen. Bedrijven kiezen voor private cloud wanneer ze meer controle over hun omgeving wensen, in ruil voor de flexibiliteit en schaalbaarheid van de public cloud.

RANSOMWARE

Ransomware is malware die de bestanden op het systeem van een slachtoffer versleutelt, waardoor deze hier niet meer bij kan. De criminelen eisen vervolgens losgeld in ruil voor de sleutel, meestal in de vorm van bitcoins of een andere cryptomunt. Daarbij zetten ze vaak extra drukmiddelen in, zoals het stapsgewijs definitief verwijderen van data zolang het slachtoffer niet betaalt. Ransomware-aanvallen kunnen ernstige financiële en operationele gevolgen hebben, waarbij slachtoffers vaak voor de moeilijke beslissing staan of ze het losgeld moeten betalen of moeten proberen hun gegevens te herstellen. Voor criminelen is ransomware buitengewoon lucratief en daarom populair. Beruchte voorbeelden uit het verleden zijn WannaCry, Petya en NotPetya.

TD SYNNEX

SECURE ACCESS SERVICE EDGE (SASE)

Secure Access Service Edge is een netwerkarchitectuur die wide-area Networking (WAN) mogelijkheden en netwerkbeveiligingsdiensten combineert in een verenigde cloud-gebaseerde oplossing. SASE integreert onder meer netwerkfuncties zoals veilige webgateways, firewall-as-a-service, zero-trust netwerktoegang en preventie van gegevensverlies om veilige toegang te bieden tot toepassingen en gegevens vanaf elke locatie, ongeacht de locatie of het apparaat van de gebruiker.

SECURITY

Security is het vakgebied gericht op het beveiligen van de ICT op alle niveaus. Het is een zeer brede discipline die zich niet alleen richt op het technisch beveiligen van systemen en netwerken, maar ook op vraagstukken als het gedrag en bewustwording bij medewerkers.

SECURITY AS A SERVICE (SAAS OF SECAAS)

Security as a Service is een model waarbij een dienstverlener security aanbiedt op basis van een cloudmodel. Deze dienst wordt op abonnementsbasis aangeboden. De dienstverlener neemt ook het complete beheer op zich, inclusief de updates.

SECURITYASSESSMENT

Een securityassessment is een grondige technische controle die inzicht biedt in de beveiligingsstatus van het ICT-netwerk. Zo ontstaat een gedetailleerd beeld van de beveiligingsrisico's en de maatregelen die nodig zijn om die risico's te mitigeren.

SECURITYAWARENESSTRAINING

Opleidings- en trainingsprogramma's voor werknemers om hen bewust te maken van IT-beveiligingsrisico's en beste praktijken. Een securityawarenesstraining bevordert de kennis over informatieveiligheid en hoe incidenten voorkomen kunnen worden. Medewerkers krijgen begrip van de mogelijke dreigingen en de impact van eventuele aanvallen op het bedrijf en het personeel. Ook worden ze geïnformeerd over het beleid en de procedures van het bedrijf voor het werken met informatietechnologie.

SECURITY-INCIDENT

Een security-incident is een gebeurtenis die de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar brengt of kan brengen. Voorbeelden van beveiligingsincidenten zijn
Denial of Service-aanvallen, besmettingen met malware en diefstal of verlies van data of hardware.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

SIEM is een datagedreven aanpak van security waarbij een centraal systeem gegevens uit verschillende bronnen haalt en hier verbanden tussen legt. Agents verzamelen de gegevens uit systemen als firewalls, antivirus, de servers, de endpoints en de netwerkapparatuur, en SIEM analyseert deze om een compleet beeld te schetsen. Het doel is om afwijkingen sneller op te merken, maar ook om het aantal false positives terug te dringen.

TD SYNNEX

SECURITY OPERATIONS CENTER (SOC)

Een SOC kan alle computer- en netwerkactiviteiten monitoren binnen een bedrijf. Vanuit een SOC houden ICT-beveiligers de omgevingen die ze moeten beschermen constant in de gaten. Op basis van een constante stroom gegevens kunnen ze reageren op ieder mogelijk security- incident. Vooral organisaties met grote hoeveelheden gevoelige data maken gebruik van SOC's. Een SOC kan in eigen beheer zijn of worden uitbesteed aan een derde partij.

SECURITYPOLICY

Een securitypolicy - of beveiligingsbeleid - geeft op een gestructureerde manier weer hoe een organisatie waardevolle assets beschermt. Een dergelijke policy omvat bijvoorbeeld het wachtwoord- en firewallbeleid, maar ook wie toegang krijgt tot welke websites, systemen en processen, op welke manier data worden opgeslagen, wie er op het draadloze netwerk van het bedrijf mag, et cetera.

SINGLE SIGN-ON (SSO)

Single Sign-On (SSO) is een techniek voor gebruikers- en sessieauthenticatie. Gebruikers krijgen via één aanmeldprocedure meteen toegang tot verschillende applicaties. Software met SSO-functionaliteit slaat meerdere identiteiten en authenticatiesleutels op en vertaalt deze naar de juiste mechanismen voor de verschillende systemen of diensten.

SMISHING

Smishing is een vorm van cybercriminaliteit die via SMS verstuurd wordt. Het woord smishing komt voort uit phishing en sms.

Smishing is een specifieke vorm van phishing. Phishing is het 'hengelen' naar persoonlijke gegevens van mensen. Het is een vorm van cybercrime waarbij criminelen je een sms sturen om te proberen inloggegevens, creditcardinformatie, pincodes of andere persoonlijke gegevens van jou te achterhalen. Hiermee willen ze geld van jou (en soms ook van je bedrijf) stelen.

SOCIAL ENGINEERING

Social engineering is gericht op misleiding van de zwakste schakel: de mens. Aanvallers maken gebruik van menselijk vertrouwen, nieuwsgierigheid of angst via methoden als imitatie, voorwendselen of lokkertjes om ongeoorloofde toegang te krijgen.
Via bijvoorbeeld phishingmails, social media of telefoongesprekken proberen internetcriminelen slachtoffers vertrouwelijke gegevens te ontfutselen, of zover te krijgen dat ze bijvoorbeeld malware installeren of op links naar kwaadaardige website klikken.

SOFTWARE-DEFINED WIDE AREA NETWORK (SD-WAN)

Een SD-WAN is een benadering voor software defined networking (SDN) technologie dat toegepast wordt op wide area network (WAN) connecties. SD-WAN maakt het makkelijker voor bedrijven om individuele bedrijfslocaties aan het interne netwerk te verbinden.

SPEARPHISHING

Spearphishing is een vorm van phishing die is gericht op specifieke personen of organisaties.

Cybercriminelen sturen mails waarin ze zich voordoen als iemand anders. Zo proberen ze hun slachtoffer op een link te laten klikken of een kwaadaardig bestand te laten openen. Het doel is om informatie buit te maken, of om malware te installeren.

SQL-INJECTIE

Een techniek die wordt gebruikt om kwetsbaarheden te misbruiken in webapplicaties die de input van gebruikers niet goed valideren. Aanvallers injecteren kwaadaardige SQL-statements in de database van een webtoepassing, waardoor zij mogelijk ongeoorloofde toegang krijgen of gegevens kunnen manipuleren.

SUPPLY-CHAIN ATTACK

Aanval op de toeleveringsketen: Gericht op kwetsbaarheden in de toeleveringsketen van software om vertrouwde producten of diensten in gevaar te brengen. Aanvallers infiltreren en knoeien met software-updates, distributienetwerken of componenten van derden, waardoor zij ongeoorloofde toegang krijgen tot gerichte systemen.

TOEGANGSCONTROLE

De praktijk van het reguleren en beperken van gebruikerstoegang tot bronnen of systemen op basis van hun rollen, machtigingen of andere authenticatiefactoren. Toegangscontrole voorkomt ongeautoriseerde toegang en beschermt gevoelige informatie.

TROUBLESHOOTING

Troubleshooting is een systematische aanpak voor het oplossen van problemen met computersystemen. De eerste stap is meestal het identificeren van het probleem, gevolgd door het bepalen en implementeren van een oplossing voor het probleem.

TWO-FACTOR AUTHENTICATION/ TWEEFACTORAUTHENTICATIE (2FA)

Bij tweefactorauthenticatie wordt de identiteit van de gebruiker van een computersysteem vastgesteld aan de hand van twee verschillende factoren. De gebruiker moet inloggen met iets wat hij weet (zoals een wachtwoord) en iets wat een gebruiker heeft (bijvoorbeeld een token of een aparte mobiele applicatie) of wat hij of zij is (biometrische kenmerken, zoals een vingerafdruk of irisscan).

VEILIGE CODEERPRAKTIJKEN

Ontwikkelingsmethoden en coderingstechnieken die erop gericht zijn kwetsbaarheden in software te minimaliseren en het risico van uitbuiting te verminderen. Veilige codeerpraktijken omvatten invoervalidatie, goede foutafhandeling en bescherming tegen veel voorkomende aanvalsvectoren.

VIRTUAL PATCHMANAGEMENT

Virtueel patchen is een proces waarbij bekende beveiligingsfouten onmiddellijk worden aangepakt (zelfs voordat een patch van de leverancier beschikbaar is) om te voorkomen dat er misbruik van wordt gemaakt en waarbij de code later wordt hersteld.

TD SYNNEX

VULNERABILITY

In de context van informatietechnologie is een kwetsbaarheid (of vulnerability) een fout in de code of het ontwerp die zorgt voor een zwakte in de beveiliging van een endpoint of het netwerk. Cybercriminelen kunnen kwetsbaarheden misbruiken voor bijvoorbeeld het uitvoeren van code of het binnendringen van een systeem.

WANNACRY

WannaCry is een ransomwareworm die zich verspreidt via kwetsbaarheden in het Windows-besturingssysteem. Bij een uitbraak van deze ransomwareworm in 2017 werden meer dan 230.000 computers in 150 landen besmet. WannaCry maakte gebruik van Eternal Blue, een exploit die door de Amerikaanse geheime dienst NSA is ontwikkeld en daar vervolgens werd gestolen.

WEB APPLICATION FIREWALL (WAF)

WAF is een beveiligingsoplossing die is ontworpen om webtoepassingen te beschermen tegen verschillende soorten cyberdreigingen, zoals SQL-injectie, cross-site scripting (XSS) en DDoS-aanvallen (Distributed Denial-of-Service). Het bevindt zich tussen de webapplicatie en de client, inspecteert inkomend en uitgaand verkeer en past een reeks vooraf gedefinieerde regels toe om kwaadaardige activiteiten te identificeren en te blokkeren, waardoor de applicatie en haar gegevens worden beschermd.

WHITELISTING

Whitelisting is een proces of praktijk waarbij specifieke entiteiten of items bevoorrechte toegang of toestemming krijgen om bepaalde acties uit te voeren binnen een systeem of netwerk. Hierbij wordt een lijst opgesteld van goedgekeurde of vertrouwde items, zoals IP-adressen, e-mailadressen of softwareprogramma's, die toegang krijgen of bepaalde activiteiten mogen uitvoeren. Door whitelisting toe te passen, krijgen alleen vooraf goedgekeurde entiteiten toestemming, terwijl alle andere automatisch de toegang wordt geweigerd of de toegang tot bepaalde functies wordt beperkt, wat een extra laag van beveiliging en controle oplevert.

ZERO TRUST

Zero Trust is een beveiligingskader dat uitgaat van geen vertrouwen tussen gebruikers, apparaten of netwerken, zowel binnen als buiten de grenzen van een organisatie. Het legt de nadruk op continue verificatie en strikte toegangscontroles, waarbij authenticatie en autorisatie vereist zijn voor elke toegangspoging, ongeacht de locatie van de gebruiker of het netwerk waarmee hij verbonden is. Zero Trust heeft tot doel het potentiële aanvalsoppervlak te minimaliseren en de risico's van bevoorrechte toegang en zijwaartse bewegingen binnen een netwerk te beperken.

ZERO-DAY KWETSBAARHEDEN

Veiligheidslekken in software of systemen die nog onbekend zijn bij de verkoper of ontwikkelaars. Cybercriminelen kunnen deze kwetsbaarheden misbruiken voordat er patches of updates zijn uitgebracht, waardoor ze zeer waardevol zijn voor het lanceren van gerichte aanvallen.

TD SYNNEX

Wil je weten waarmee we je kunnen helpen? Neem dan contact op met ons security team.

Tel: +31 (0) 250 27 07
Email: tdsecurity@tdsynnex.nl
www.connect.tdsynnex.nl/solution/security/